

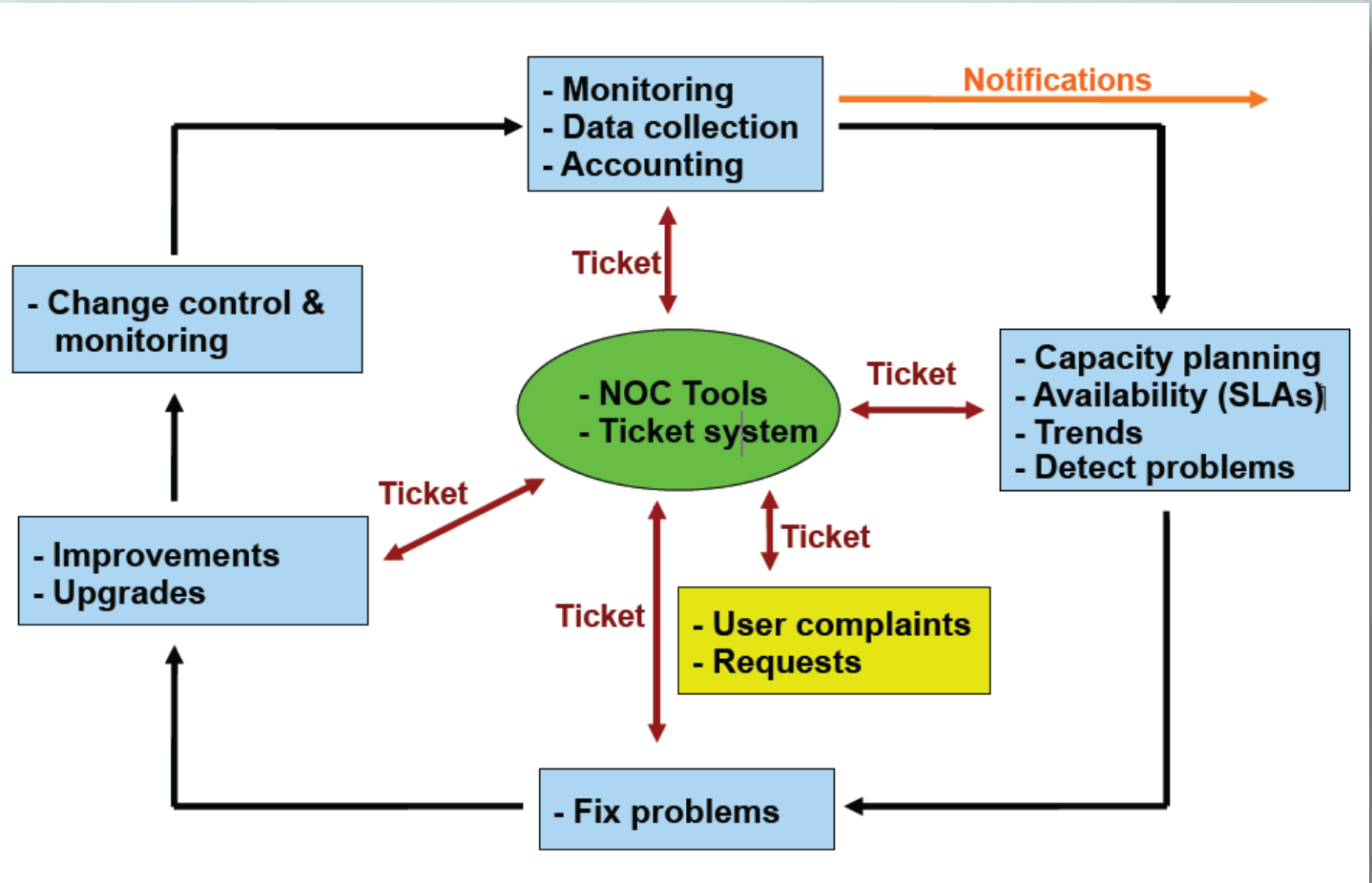
Network Management

Automated Intelligence

GZ Kabir
BDCOM ONLINE LTD.

- Network Management
 - Parameters
 - Components
 - Tools
 - Demonstration

How should we manage



- **Operation:**

keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

- **Administration:**

deals with keeping track of resources in the network and how they are assigned.

- **Maintenance:**

concerned with performing repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run "better".

- **Provisioning:**

is concerned with configuring resources in the network to support a given service.

Network Management is the use of a system that constantly monitors a computer network for slow or failing systems and that notifies the network administrator in case of outages via email, SMS or other alarms.

subset of the functions involved in network management.

Network Management

- System & Service monitoring
 - Reachability, availability
- Resource measurement/monitoring
 - Capacity planning, availability
- Performance monitoring (RTT, throughput)
- Stats & Accounting/Metering
- Fault Management
 - Fault detection, troubleshooting, and tracking
- Configuration/Change Management
- Coordination

Components

- Availability
- Reliability
- Performance
- Configuration Mgmt & Monitoring
- Network Forensic
- Intrusion Detection ...
-
-
- Coordination

- **Diagnostic tools** – used to test connectivity, ascertain that a location is reachable, or a device is up – usually active tools
- **Monitoring tools** – tools running in the background (“daemons” or services), which collect events, but can also initiate their own probes (using diagnostic tools), and recording the output, in a scheduled fashion.







- Active tools
 - Ping – test connectivity to a host
 - Traceroute – show path to a host
 - MTR – combination of ping + traceroute
 - SNMP collectors (polling)
- Passive tools
 - log monitoring, SNMP trap receivers
- Automated tools
 - SmokePing – record and graph latency to a set of hosts, using ICMP (Ping) or other protocols
 - MRTG – record and graph bandwidth usage on a switch port or network link, at regular intervals
 - So **MANY** More

Tools ... Availability

- Nagios
 - server and service availability monitoring
 - Can monitor pretty much anything
 - HTTP, SMTP, DNS, Disk space, CPU usage, ...
 - BGP, OSPF, Switch Port, room temperature, ..
 - Easy to write new plugins (extensions)
- Zabbix, ZenOSS, Hyperic, ... Many more Open Source...
- Log, Log, Log
- Notification mechanism

Tools Nagios

Corporate Client (Corporate Client)

Host	Status	Services	Actions
ITDG	UP	1 OK	  
berger	UP	1 OK	  

Cisco-Mikrotik (Router)

Host	Status	Services	Actions
bdix	UP	2 OK	  
bttb_main	UP	1 OK	  
corerouter	UP	3 OK	  
corerouter smile	UP	3 OK	  
ctqgw	UP	2 OK	  
qlsgw_router	UP	2 OK	  
motiheelaw_router	UP	1 OK	  
panthagw_router	UP	1 OK	  
syihet_router	UP	1 OK	  

Linux Servers (linux-servers)

Host	Status	Services	Actions
bbgw10	UP	2 OK	  
bbgw20	UP	1 OK	  
bbgw30	UP	1 OK	  
bdoom_maxim_billing	DOWN	1 CRITICAL	  
ctq_dist	UP	1 OK	  
digium	UP	1 OK	  
dns1	UP	1 OK	  
dns2	UP	1 OK	  
dns3	UP	1 OK	  
dslgw	UP	1 OK	  
dslgw2	UP	1 OK	  
qls	UP	1 OK	  
hardy	UP	1 OK	  
iptalkG2	UP	1 OK	  
localhost	UP	3 OK	  
mail.com	UP	4 OK 1 WARNING	  
mail.net	UP	5 OK	  
motiheel distribution	UP	1 OK	  
pantha_dist	UP	2 OK	  
shout_share	UP	1 OK	  
smtp	UP	2 OK 1 CRITICAL	  

Nagios[®]

Tools Nagios

Network Map For All Hosts
Last Updated: Fri Jan 11 11:50:18 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - www.nagios.org
Logged in as nagiosadmin

[View Status Detail For All Hosts](#)
[View Status Overview For All Hosts](#)

Layout Method:

Circular

Scaling factor:

0.0

Drawing Layers:

Environmental Probes
Fedora Core 8 Production Servers
Printers
Production Linux Servers

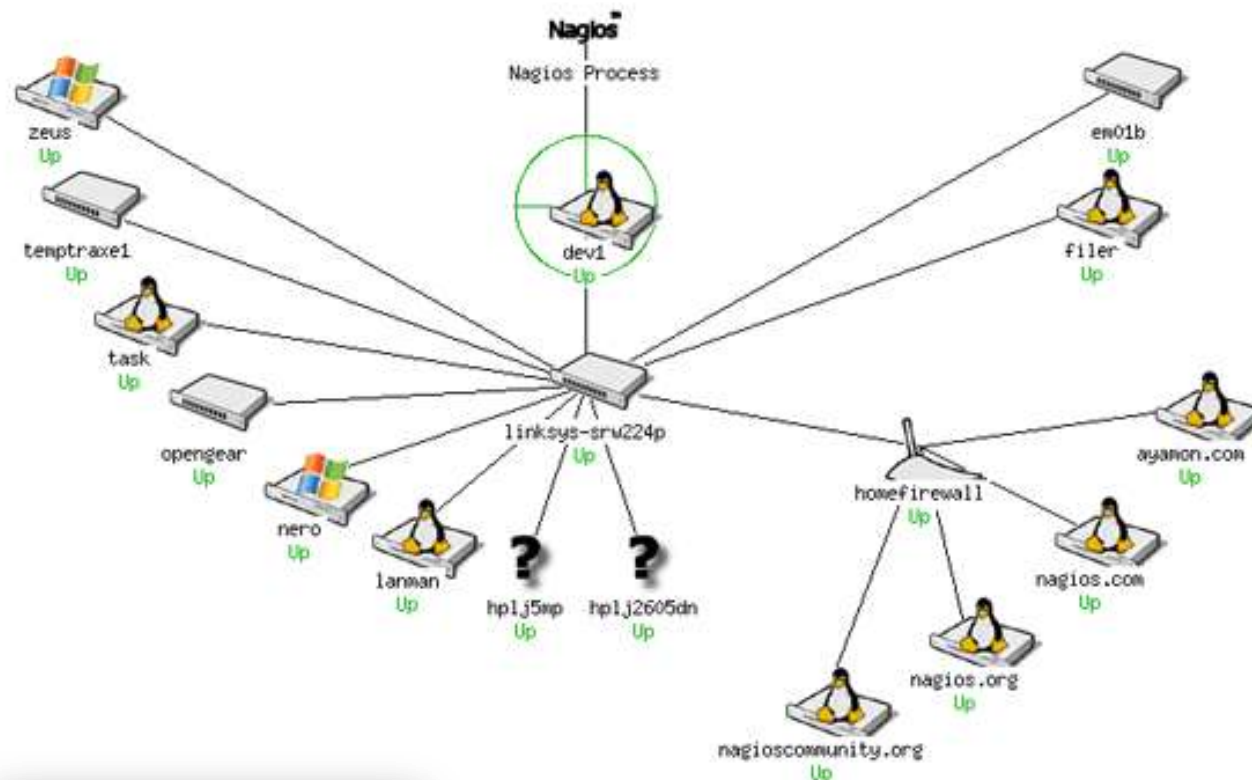
Layer mode:

Include
 Exclude

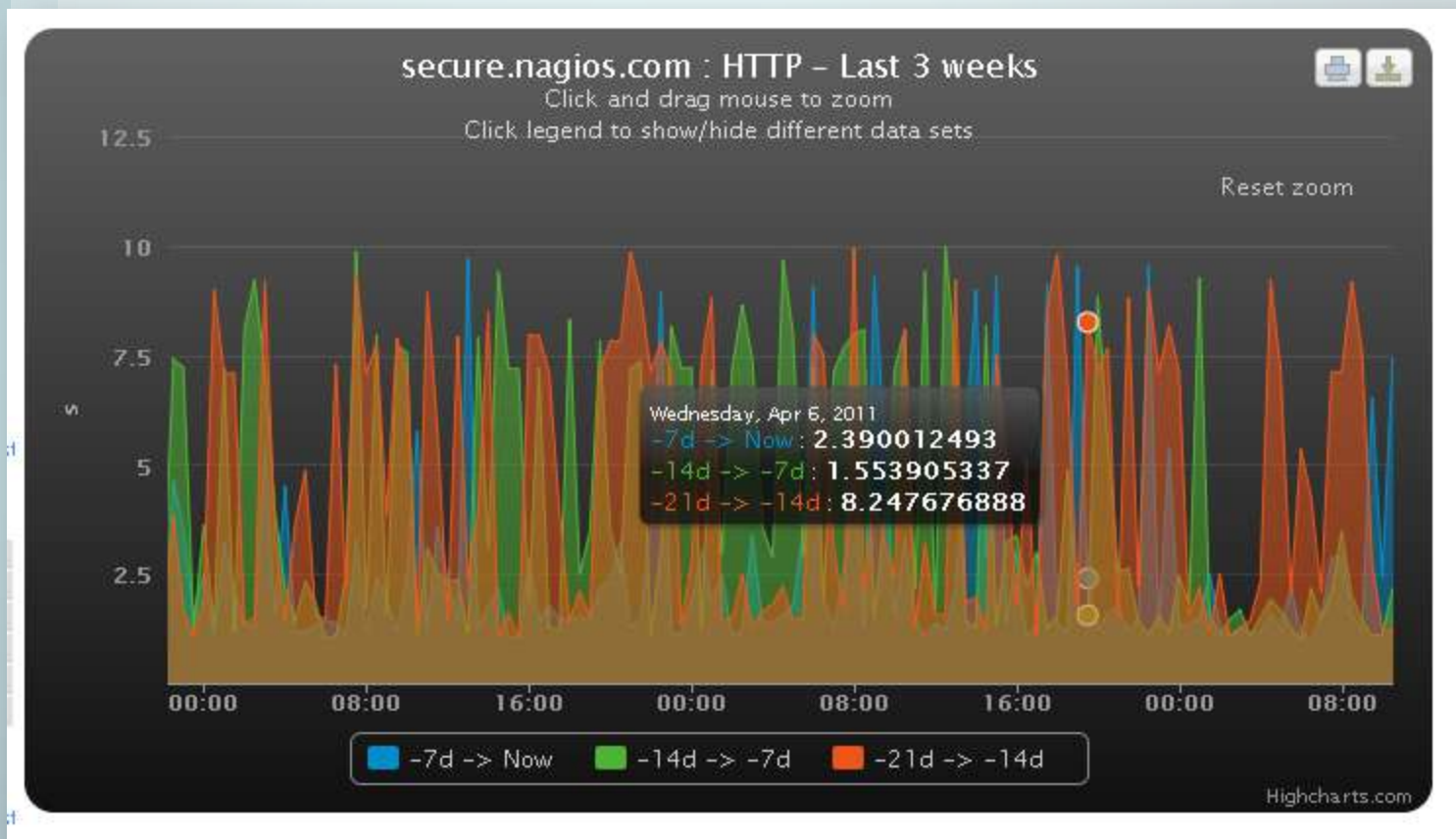
Suppress popups:

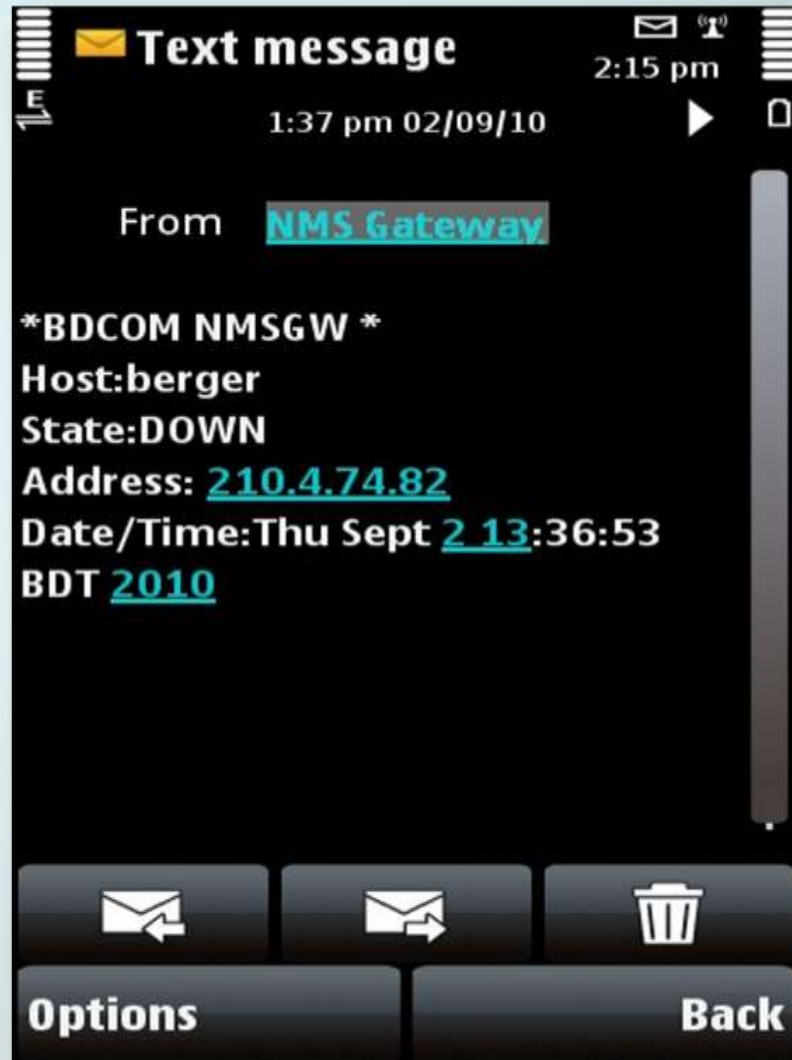


Update



Nagios®





□ SmokePing

- Keeps track of your network latency:
- Best of breed latency visualisation.
- Interactive graph explorer.
- Wide range of latency measurement plugins.
- Master/Slave System for distributed measurement.
- Highly configurable alerting system.
- Live Latency Charts with the most 'interesting' graphs.
- Free and OpenSource Software written in Perl

Tools ... SmokePing



SmokeTraceroute to www.switch.ch - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://loss.oetiker.ch/smokeping-demo/tr.html#www.swit

Home Places Gedafe Google JS Dict RRD

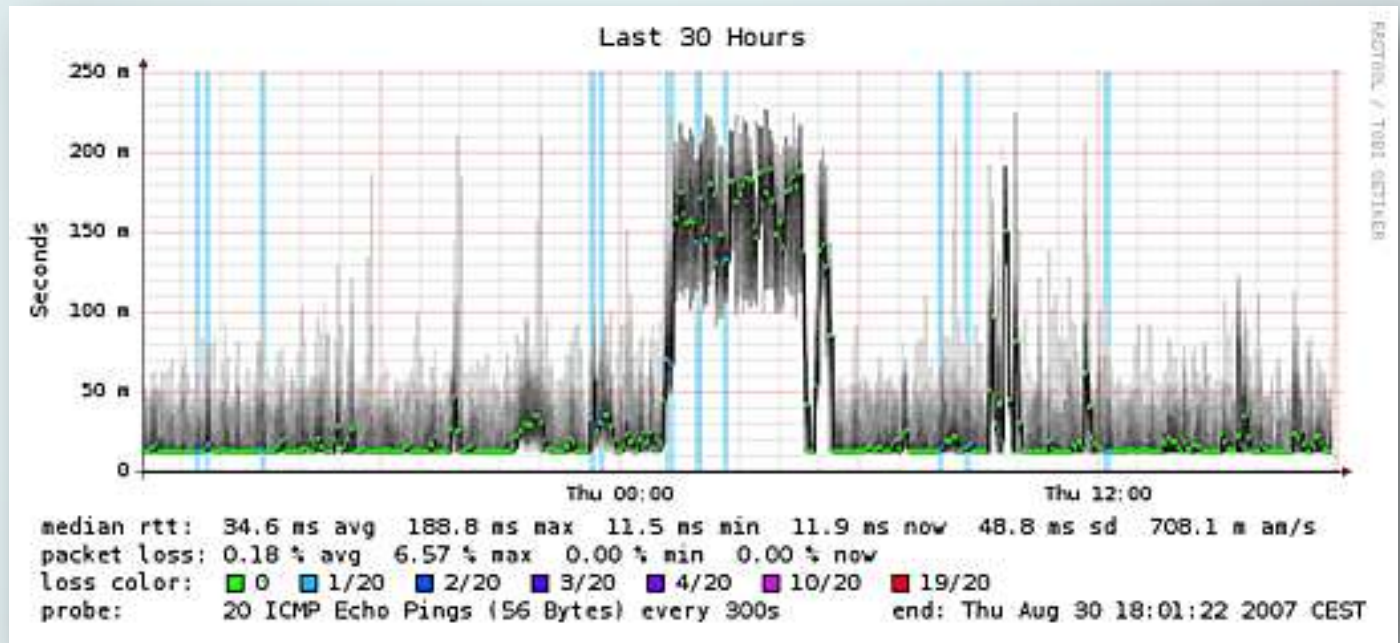
SmokeTrace Host Delay Rounds Go

Hop	Host	ip	Loss [%]	Sent	Last [ms]	Avg [ms]	Best [ms]	Worst [ms]	StDev [ms]
1.0	r4.core.int7.net	213.144.138.193	0 %	20	122.8	7.6	0.3	122.8	27.4
2.0	r1zur1.core.int7.net	77.109.128.49	0 %	20	7.9	3.0	0.5	9.6	2.9
3.0	swiIX1-10GE-1-2.switch.ch	194.242.34.53	0 %	20	1.7	1.2	0.7	1.8	0.3
4.0	swiZH2-10GE-1-3.switch.ch	130.59.36.130	0 %	20	1.1	1.2	0.9	1.6	0.2
5.0	swiEL2-G2-3.switch.ch	130.59.36.78	0 %	20	4.1	4.5	3.7	10.5	1.4
6.0	swiAM2-10GE-1-4.switch.ch	130.59.36.10	0 %	20	3.9	4.0	3.6	4.5	0.2
7.0	oreus.switch.ch	130.59.138.34	0 %	20	3.6	3.8	3.4	4.3	0.2

SmokeTrace is part of the SmokePing suite created by Tobi Oetiker, Copyright 2008.

Done: 8,324 - 148 - \$25.76

Tools ... SmokePing

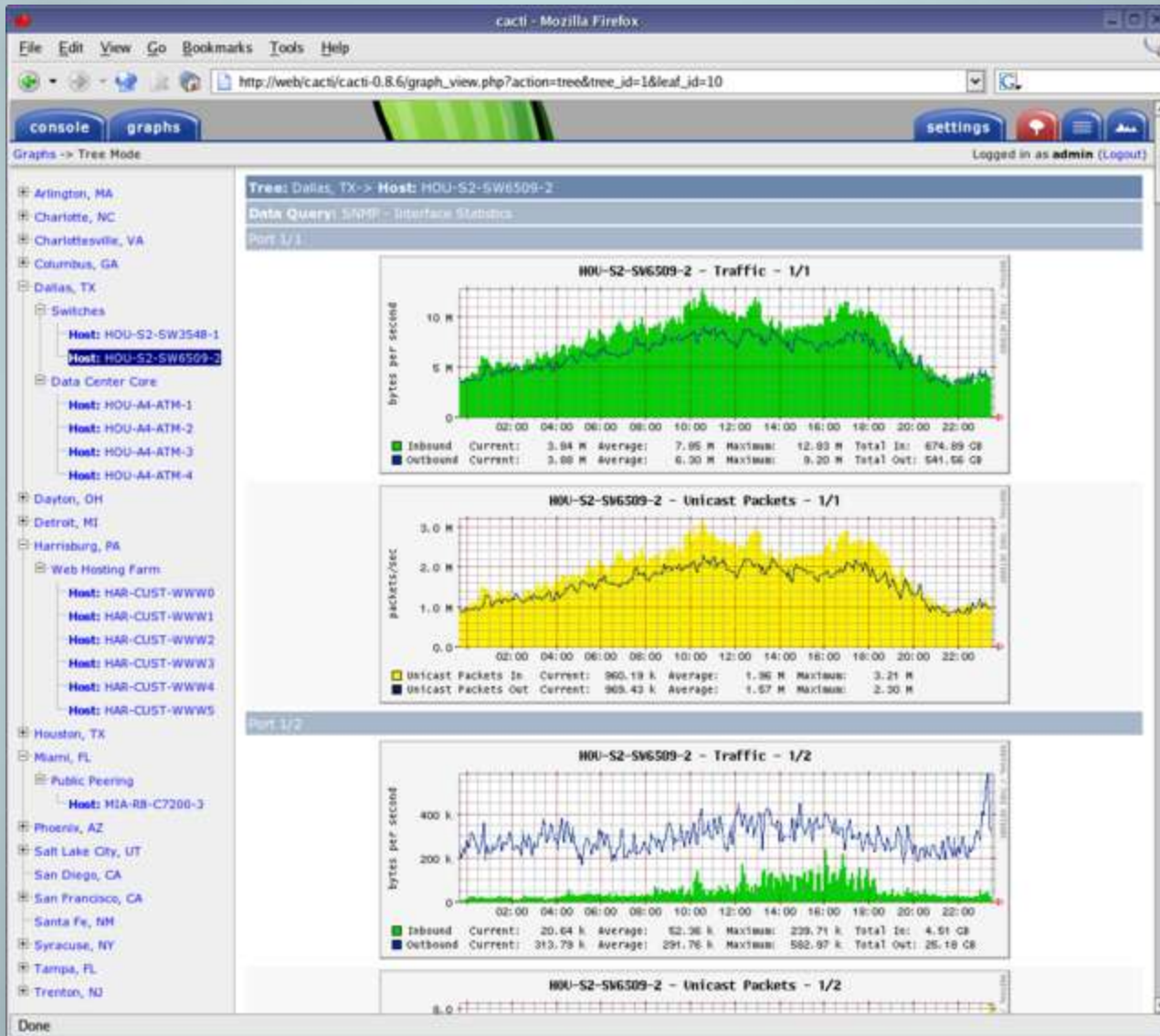




□ Cacti/MRTG

- A tool to monitor, store and present network and system/server statistics
- Designed around RRDTool with a special emphasis on the graphical interface
- Almost all of Cacti's functionality can be configured via the Web.
- Uses RRDtool, PHP and stores data in MySQL
- Supports the use of SNMP and graphics with MRTG
- Authentication Scheme
- Large Network Deployment

Tools ... Cacti



Tools ... Weathermap

File Edit View Go Bookmarks Tools Help

http://localhost/cacti/plugins/weathermap/weathermap-cacti-plugin.php

Disable* Cookies* CSS* Forms* Images* Information* Miscellaneous* Outline* Resizer* Tools* View Source* Options*

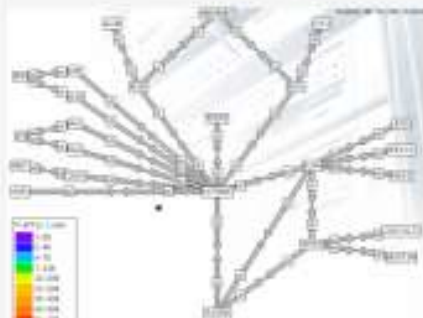
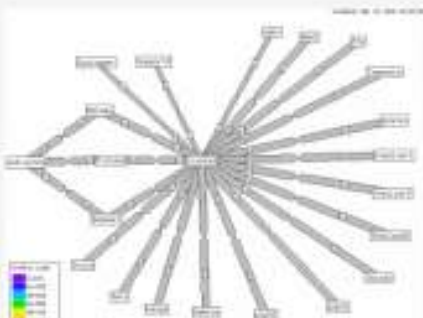
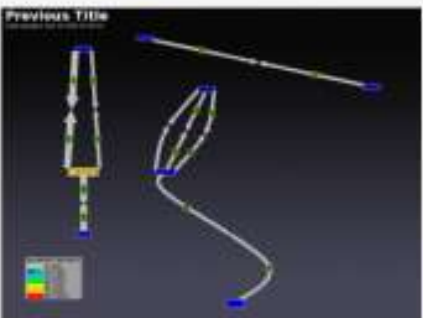
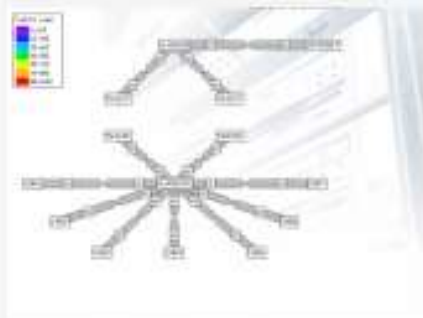
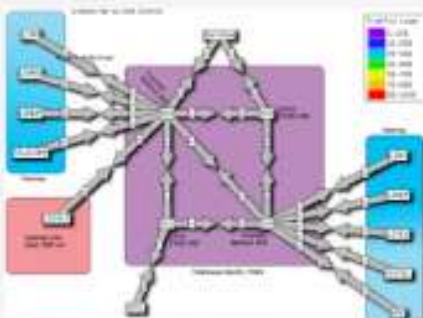
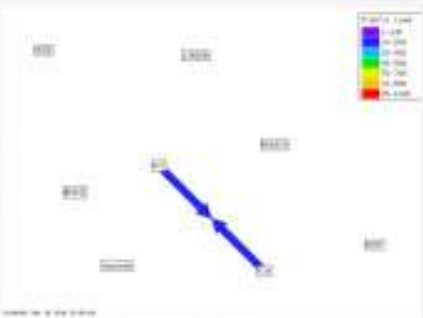

HJNews Admin Time:Piece - Object Oriented time ... Petal: Cookbook - Recipes for build... Petal - Ped Template Attribute Lang... Petal:Utils - Useful template modifi... Howie's Stuff:Network Stuff:Links ... Management -> Devices view else ... Howie's Stuff:Network Stuff:PHP... cacti

console graphs threshid monitor discover weathermap Devices settings

Console - Weathermap logged in as admin (Logout)

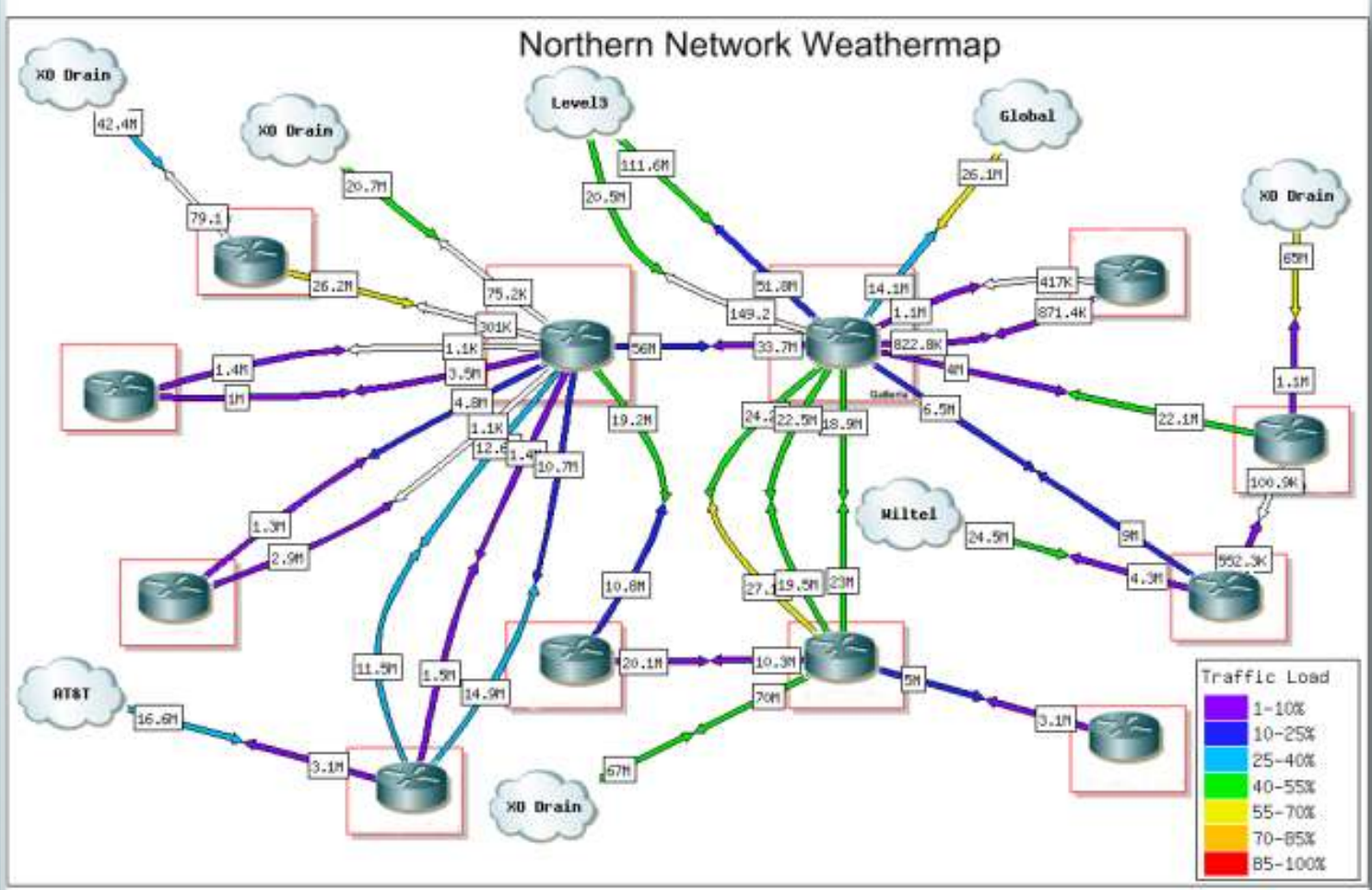
Network Weathermaps [Manage Maps](#)

Click on thumbnail for a full view

<p>Network Weathermap</p> 	<p>Internet Servers</p> 	<p>Previous Title</p> 
<p>Network Weathermap</p> 	<p>Network Weathermap</p> 	<p>Network Weathermap</p> 
<p>UK Network Overview</p> 		

Done

Tools ... Weathermap



The "Really Awesome New Cisco config Differ"

- Rancid
 - Rancid is a configuration management tool that keeps track of changes in the configurations of any size network equipment (Cisco, HP, Juniper, Foundry, etc.). Works on routers and switches. Automates retrieval of the configurations and archives them as backup tool, audit tool, blame allocation.

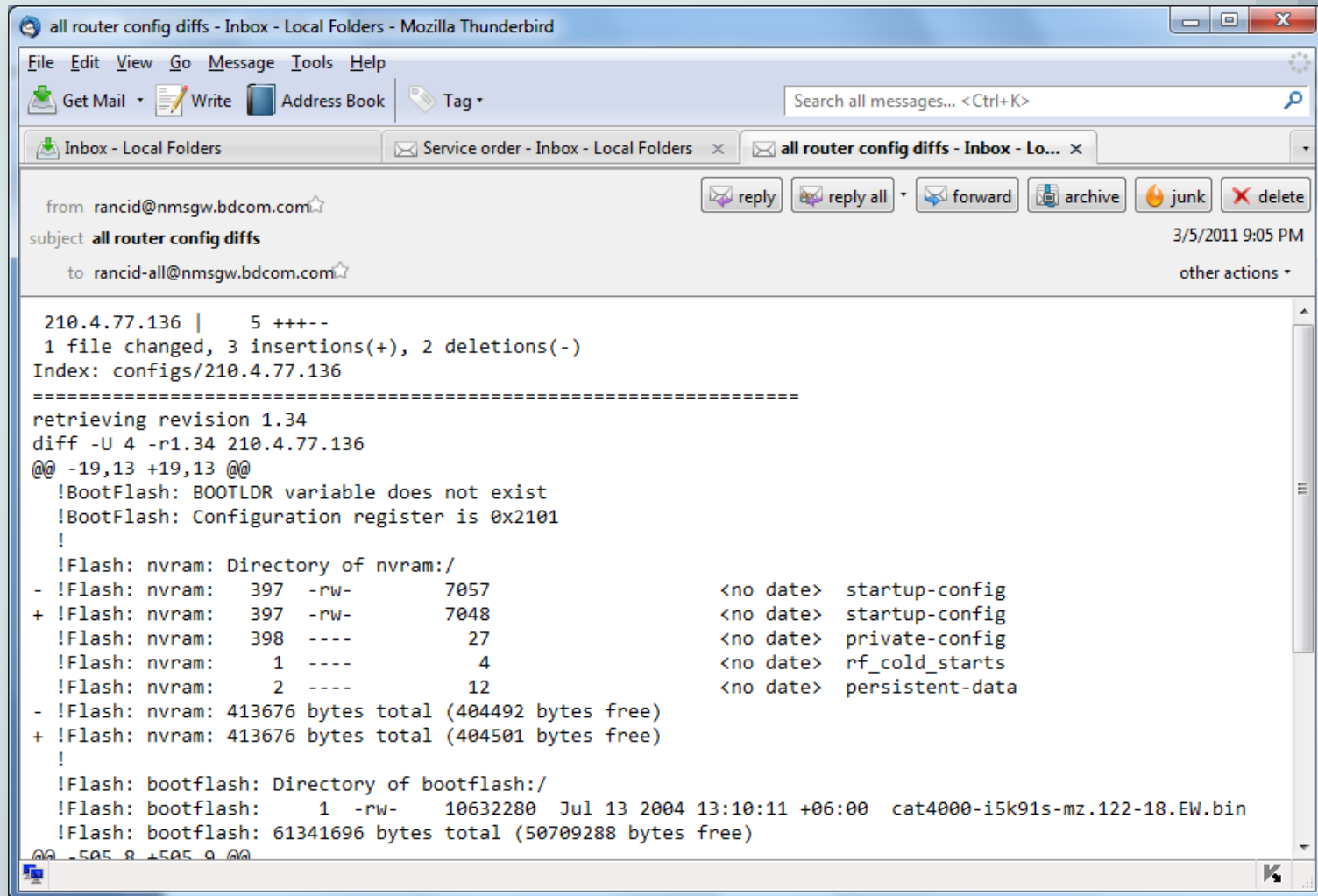
The "Really Awesome New Cisco config Differ"

□ Rancid

The data is stored in a VCS (Version Control System) which keeps

- Track changes in the equipment configuration
- Track changes in the hardware (S/N, modules)
- Track version changes in the OS (IOS, CatOS versions)
- Find out what your colleagues have done without telling you!
- Recover from accidental configuration errors .

Tools ... Rancid



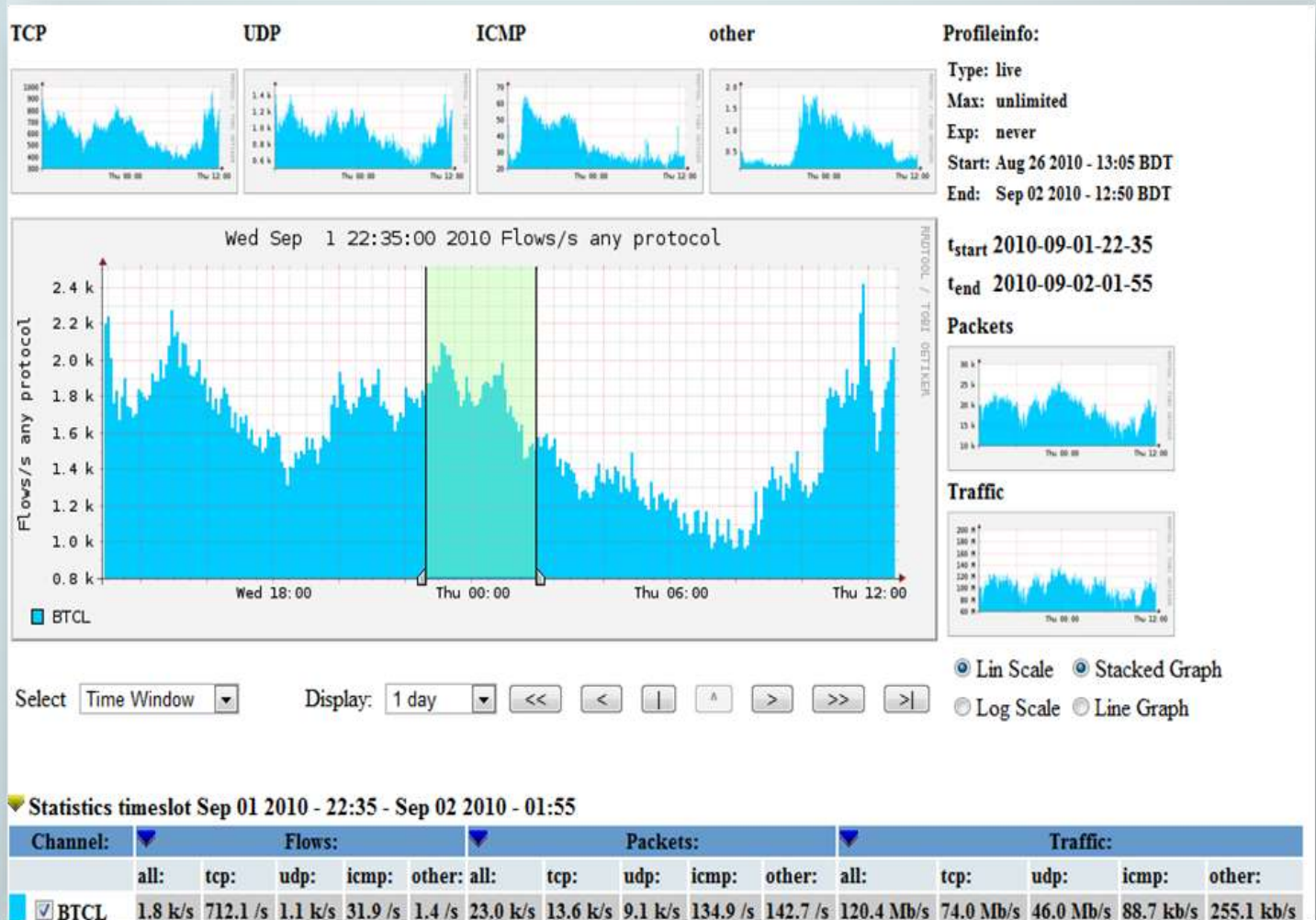
□ **Network Flow Analysis Tool**

- NetFlow (C),
- cflowd (F),
- FlowScan (F),
- Sniffer Pro (C),
- argus (F),
- i-Flow (C)
- NFSen (F)

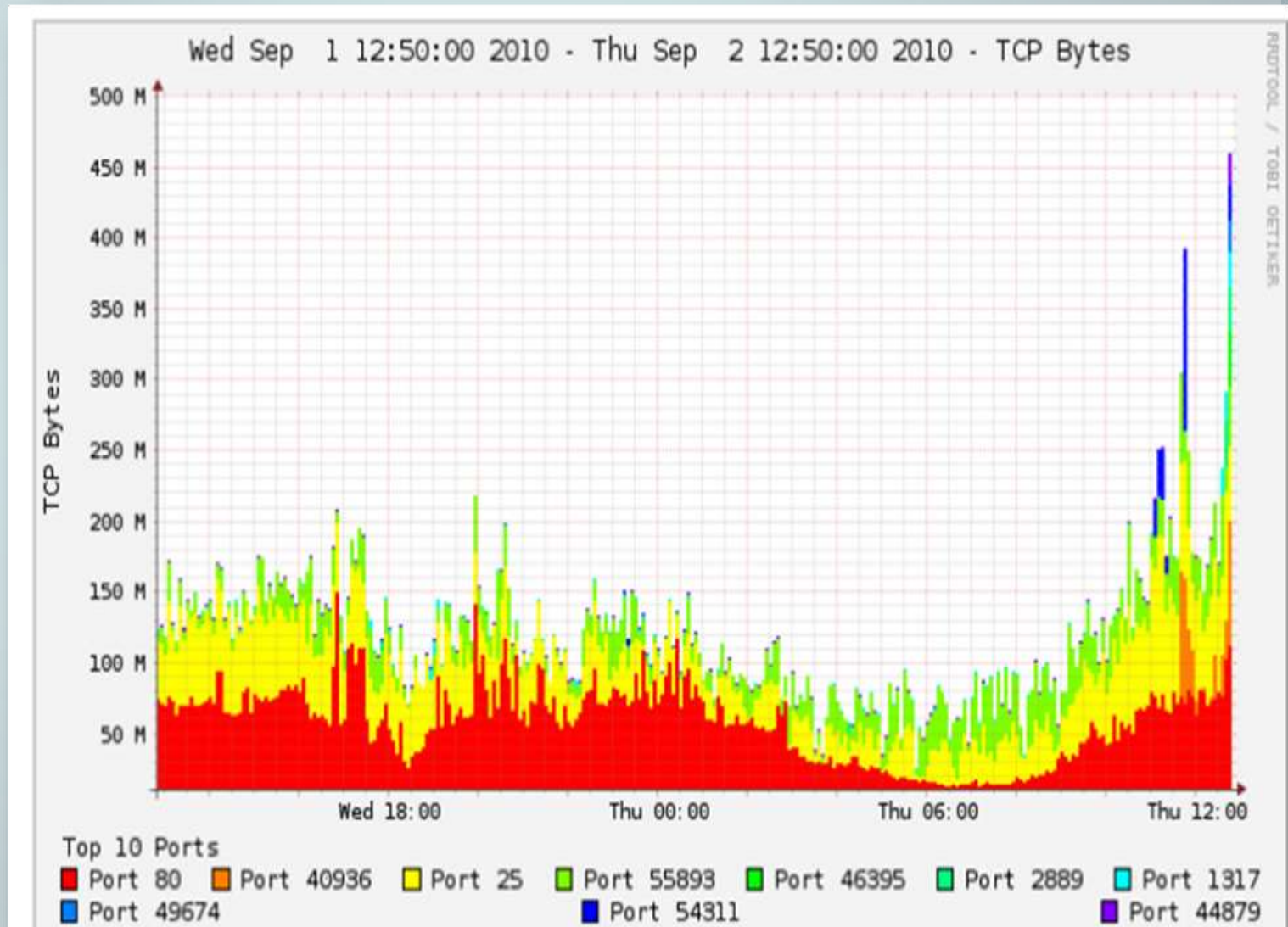
□ Network Flow Analysis Tool

■ NfSen

- Display netflow data: Flows, Packets and Bytes using RRD (Round Robin Database).
- Easily navigate through the netflow data.
- Process the netflow data within the specified time span.
- Create history as well as continuous profiles.
- Set alerts, based on various conditions.



Tools ... NfSen



Rank	TCP						UDP						
	Flows		Packets		Bytes		Flows		Packets		Bytes		
Port	Count	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count
1	80	39029	80	570630	80	111021671	53	116671	53	150335	12610	142186426	
2	445	27833	25	83140	40936	88004359	6881	2388	12610	99433	28712	101344390	
3	135	24572	40936	66203	25	52612168	39792	2276	28712	70901	40493	93146942	
4	25	7881	445	53175	55893	43525223	15507	1904	40493	65155	46886	27824516	
5	23	6761	135	49066	46395	39079355	43040	1611	15699	46682	57563	26436088	
6	3128	4786	55893	37615	2889	30261886	60928	1588	1416	40540	62390	25767022	
7	443	2999	46395	35068	1317	24692504	51012	1573	57563	37794	54505	25550351	
8	22	2517	22	27489	49674	23472247	61295	1447	34018	37747	55893	23548341	
9	9415	1275	443	26468	54311	23342821	5060	1309	21694	24942	40633	22940400	
10	8080	1081	21651	25614	44879	23306526	49665	1225	46886	19468	40403	19544859	

Computer Security is not something that you can just add on when you need it.

Proper planning, installation, monitoring and maintenance all become part of a successful IDS/IPS implementation.

- Tri-Sentry (Host Sentry, NetSentry, Service Sentry)
- Nessus, Snort
- Checkpoint, Cisco IPS, UTM (Cyberoam, Barracuda)

BIG BOYS WILL DISCUSS

So, we have many Open Source/Commercial deployments already to monitor our network.

All the programs can generate alert/alarm on fault detection.

Need to centralize all the information.

We need to collaborate these programs

Need NOC

Its not a big Room/House – it's a software

Its –RT (the ticketing system)

Request Tracker

- RT is a battle-tested issue tracking system which thousands of organizations use for
 - bug tracking,
 - help desk ticketing,
 - customer service,
 - workflow processes,
 - change management,
 - network operations,
 - And so on ..

Request Tracker

Whenever, wherever and however there is a problem in the network the relevant monitoring software will send a ticket directly to RT system and system admins will know immediately via email or SMS. This automation will keep track of the SLA. RT has its own Help Desk system and escalation procedure.

Request Tracker

Whenever, wherever and however there is a problem in the network the relevant monitoring software will send a ticket directly to RT system and system admins will know immediately via email or SMS. This automation will keep track of the SLA. RT has its own Help Desk system and escalation procedure.

- Why are they important?
 - Track all events, failures and issues
- Focal point for help desk communication
- Use it to track all communications
 - Both internal and external
- Events originating from the outside:
 - customer complaints
- Events originating from the inside:
 - System outages (direct or indirect)
 - Planned maintenance, upgrades, etc.

Home ▾ Tickets ▾ Tools ▾ Logged in as jesse ▾ RT for example.com >> << BEST PRACTICAL™

RT at a glance New ticket in General ▾ Search...

Edit

^ 10 highest priority tickets I own Edit

#	Subject	Priority	Queue	Status
1	Office has run out of coffee!	0	Office	(pending 1 other ticket)
2	Order more coffee	0	Office	(pending 2 other tickets)

^ 10 newest unowned tickets Edit

#	Subject	Queue	Status	Created	
3	Obtain Series-C funding	General	new	52 sec ago	Take

^ Bookmarked Tickets Edit

#	Subject	Priority	Queue	Status	
4	Evaluate responses to RFP for coffee roasts	0	General	new	★

^ Quick ticket creation

Subject:

Queue: Owner:

Requestors:

Content:

[Create](#)

^ My reminders

^ Quick search Edit

Queue	new	open	stalled
General	2	-	-
Office	1	1	-

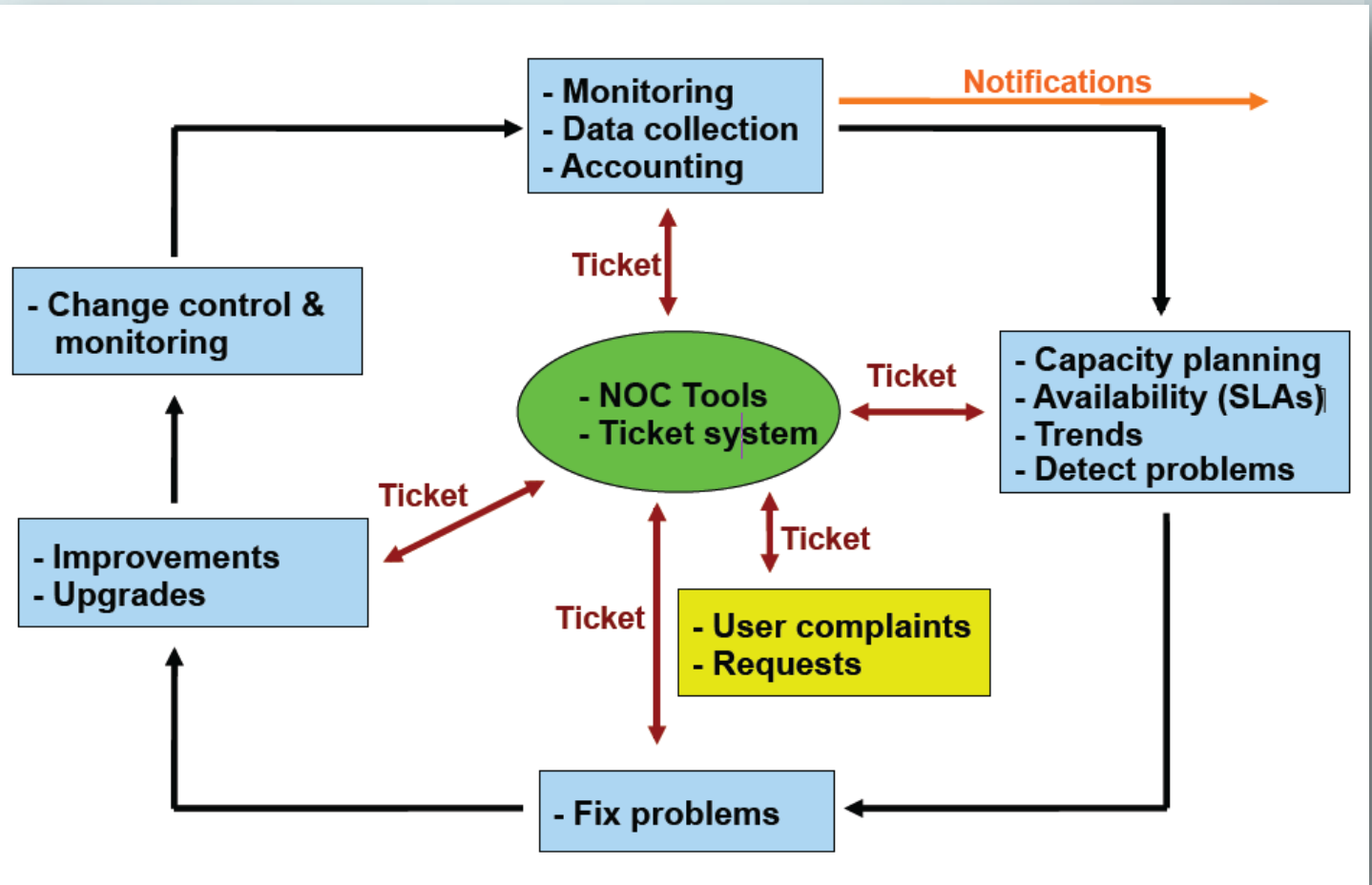
^ Dashboards Edit

RT System's dashboards	Subscription
SLA Performance	daily at 6:00 AM

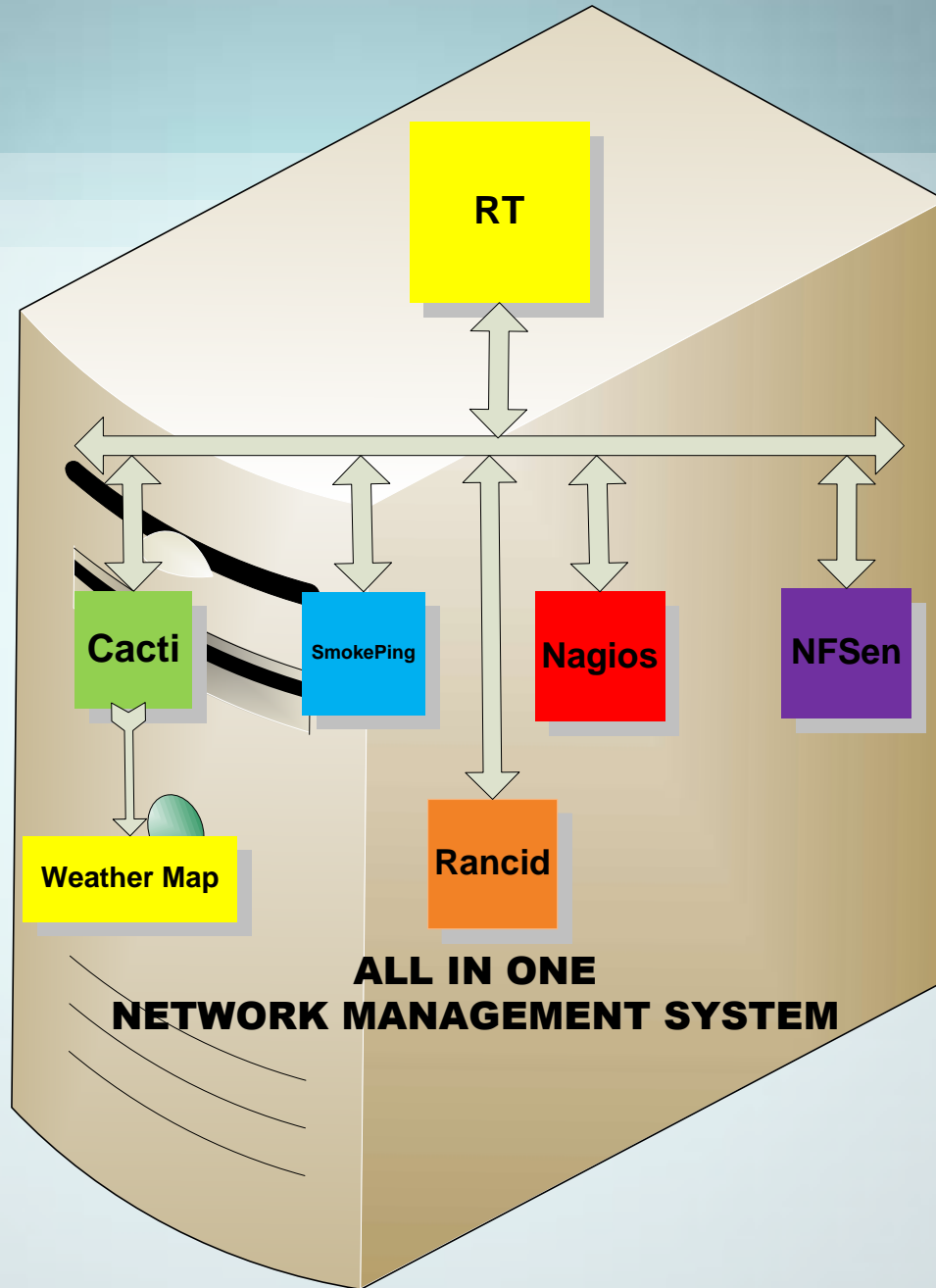
^ Refresh

Don't refresh this page. [Go!](#)

Tools ... RT



Conclusion





Thanks ...

**Very Special Thanks to
NSRC Team**